PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G11C 7/16	A1	(11) International Publication Number: WO 00/31744
		(43) International Publication Date: 2 June 2000 (02.06.00)

(21) International Application Number: PCT/GB99/03877

(22) International Filing Date: 19 November 1999 (19.11.99)

(30) Priority Data:
9825337.0 19 November 1998 (19.11.98) GB

(71) Applicant *(for all designated States except US)*: MEMORY CORPORATION TECHNOLOGY LIMITED [GB/GB]; The Computer House, Dalkeith Palace, Dalkeith, Midlothian EH22 2NA (GB).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: TAYLOR, Richard, Michael [GB/GB]; Old Sawmill House, 41 Newmills Road, Dalkeith EH22 2AQ (GB). OXLEY, David, Peter [GB/GB]; Flat 2F1, 43 St. Patrick Square, Edinburgh EH8 9ET (GB).

(74) Agents: MCCALLUM, William, Potter et al.; Cruikshank & Fairweather, 19 Royal Exchange Square, Glasgow G1 3AE (GB).

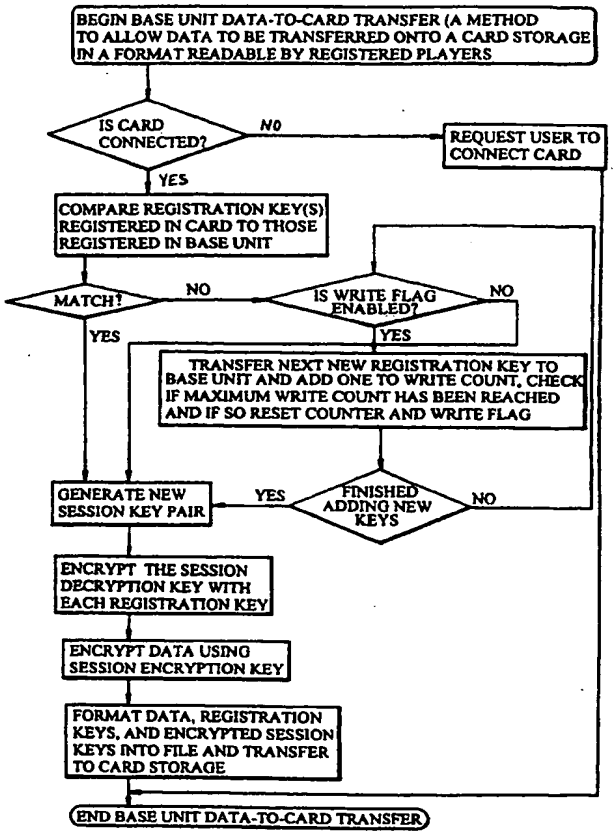
(81) Designated States: GB, JP, KR, SG, US.

Published
With international search report.

(54) Title: COPY MANAGEMENT FOR DATA SYSTEMS

(57) Abstract

The invention relates to a method of controlling unauthorised copying of data, for example copying of audio data from an original Compact Disc (CD), or copying of audio data files which have been legally purchased over a network system, for example using the Internet. In particular, although not exclusively, the invention relates to a method and apparatus for controlling unauthorised copying of music onto portable solid state memory audio player devices (2), or onto removable solid state memory cards (3) for use with such portable player devices. A data copying and playback system incorporating copy management is also claimed.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

COPY MANAGEMENT FOR DATA SYSTEMS

The present invention relates to a method of controlling unauthorised copying of data, for example copying of audio data from an original Compact Disc (CD), or copying of audio data files which have been legally purchased over a network system, for example using the Internet. In particular, although not exclusively, the invention relates to a method of controlling unauthorised copying of music onto portable solid state memory audio player devices, or onto removable solid state memory cards for use with such portable player devices.

Some past attempts at controlling copying of audio data have relied on a user entering a registration character string or number to enable a player system (e.g. a personal computer (PC) with an audio playback facility) to decode audio data which is supplied in encoded or encrypted form to the player system. Such systems are not particularly user friendly and are compromised if the user gives away the registration string or number to other parties.

Portable audio players are known which allow a user to playback music which is stored (in digital form) in a solid state memory of the player. The solid state memory may, for example, be FLASH memory incorporated in the player itself, or may be provided as a removable FLASH memory card for insertion into the player device. PCs are readily available which can be configured to enable a user to copy or "download" audio data from the Internet, or from a CD engaged in a CD-ROM drive of the computer, onto a storage medium such as a hard disk of the PC. Equipment is also available which enables a user to copy audio data stored in the hard drive of the PC into the solid state memory of a portable audio player device. The portable player device may then be used by a user to playback music at a remote location e.g. while out jogging.

In general, there is nothing to stop a user from using such

equipment to make many unauthorised copies of audio data, for example repeated copies of a single, legally purchased CD, or even many copies of an unauthorised copy of a CD which may be available for download from, for example, the Internet. This gives great concern to musicians and the music industry alike.

It is an aim of the present invention to avoid or minimise one or more of the foregoing disadvantages.

According to one aspect of the present invention we provide a method for controlling the number of data player devices which may be used for playback of data which has been copied, using a copying system, from a first data storage means accessible to the copying system in use thereof, to a second data storage means associated with the player device(s), the method comprising the steps of:

providing a copy management means to which data copied from the first data storage means is delivered;

providing a registration code for each of a plurality of data player devices, said registration codes all being different;

providing a private key for each of said data player devices, said private keys all being different;

storing a predetermined maximum number of said registration codes in a memory means of the copy management means;

using an encryption key provided in the copy management means to encrypt data delivered to the copy management means from the copying system, and using each stored registration code to encrypt a decryption key provided in the copy management means, so as to provide a plurality of respective encrypted decryption keys;

transferring the encrypted data to a second data storage means associated with at least one said player device, together with the plurality of encrypted decryption keys;

using the private key provided in said at least one player device to decrypt the respective encrypted decryption key, and using the decrypted decryption key to decrypt the encrypted data transferred to said second data storage means;

and preventing new registration codes from being stored in the memory means of the copy management means until a predetermined time period has elapsed.

One advantage of the above method is that it provides a registration scheme for player devices which limits the number of player devices which can be used at one time to listen to music which has been copied from another source, using the copying system. If only a limited number of players can be used to playback music which has been copied, this may tend to dissuade users from, for example, producing a multiplicity of copies of a single CD, and moreover even if mass copies are made, a user cannot playback the music from such a copy without using a player which was registered with the copying system when the copying was carried out.

The decryption key provided in said at least one player device may also be the encryption key used to encrypt the data being copied. Alternatively, the decryption key may be a separate key, different to the encryption key.

The private key provided in each player device may in fact be the registration code for the player device. In general, though, the private key will preferably be a separate key, different to the registration code. The advantage of this is that while the registration code may, in some cases, to some extent be accessible to a user in that it must be transferred from the player device to the second data storage means, the private key can be held in a tamper-proof location in the player device and need never be transmitted outside the player device.

According to another aspect of the invention we provide copy management apparatus for controlling the number of data player devices which may be used for playback of data which has been copied, using a copying system, from a first data storage means accessible to the copying system in use thereof, to a

second data storage means associated with the player device(s), the apparatus comprising:

memory means for storing up to a predetermined maximum number of registration codes, each said code being associated with a respective data player device;

encryption means for encrypting data delivered thereto, including an encryption key for use in carrying out the data encryption, and including encryption means for encrypting a decryption key, provided in the apparatus, using each said registration code which is stored in the memory means in order to generate a respective encrypted decryption key for each said stored registration code;

clock means for measuring the passing of a finite predetermined period of time within which new registration codes are prevented from being stored in the memory means;

monitoring means for monitoring the number of registration codes stored in the memory means and starting said clock means when said monitoring means detects that the predetermined maximum number of codes have been stored;

protection means for setting the memory means in a protected mode, in which new registration codes are prevented from being entered in the memory, while said clock means measures the passing of said finite period of time;

registration handler means for receiving at least one registration code uploaded, directly or indirectly, from at least one said data player device, comparing said at least one uploaded registration code with the registration codes already stored in the memory means, storing said at least one uploaded registration code in the memory means if the memory means does not already contain said at least one uploaded registration code and the memory means does not already contain said predetermined maximum number of registration codes, and preventing said uploaded registration code from being stored in the memory means if the memory means is set in said protected mode; and

data transfer means for transferring the encrypted data, together with each said encrypted decryption key, to a second

data storage means associated with at least one said player device.

The encrypted copied data can subsequently be accessed by a data player device associated with said second data storage means. A said data player device whose registration code is stored in the memory of the said copy management apparatus will be provided with identifier means for identifying the respective encrypted decryption key for the said data player device, and with decryption means for decrypting the encrypted decryption key and subsequently using said decrypted decryption key to decrypt the encrypted data stored in the second data storage means. The decryption means provided in the player device preferably includes a private key stored in the player device, for use in decrypting the encrypted decryption key.

The afore-described data player devices may, for example, be for playback of audio data i.e. music. Alternatively, or additionally, the player devices could, for example, be portable "electronic book" devices for playback of written data.

Preferably, said second data storage means associated with the player device(s) comprises a removable memory card which is formed and arranged for removable engagement with a complementary interface provided in data player device(s). It will be appreciated that the removable memory card need not be connected to a said player device when encrypted data is being transferred thereto, and that the card will generally be capable of interfacing with any of a number of data player devices, for example a set of player devices owned by one user, such as a portable audio player device, a home stereo system, and a car audio system. The user will also own a copying system in the form of, for example, a PC system and additional necessary equipment, for copying data (e.g. audio data) from a CD or DVD onto the removable memory card, or a

specially adapted dedicated audio dubbing station designed to copy audio data from one or more CDs or DVDs onto the removable memory card (as described in our concurrent British patent application). The memory card is therefore also formed and arranged for interfacing with such a copying system. The copying system may, alternatively, be in the form of a set-top box system designed for copying data purchased from a network supplier (e.g. cable supplier) onto the removable memory card. In the latter case it will be appreciated that the "first data storage means" will generally comprise a memory of the set-top box in which data purchased from the network supplier is downloaded from the network.

Alternatively, the second data storage means associated with the player device(s) may comprise solid state memory permanently incorporated in each said data player device and each player device is adapted for interfacing directly with the copy management apparatus to receive the encrypted data transferred therefrom.

The monitoring means preferably comprises counter means for counting the number of registration codes which are written to the memory means. The registration handler means is preferably formed and arranged to check the status of the counter means, upon receiving an uploaded registration code, and to allow or prevent the uploaded registration code from being written in the memory means according to whether the counter means indicates that the memory means already contains said predetermined maximum number of stored registration codes or not, respectively.

The encryption (and/or decryption key, where this is not the same as the encryption key) may be selected from a predetermined list of encryption and/or decryption keys stored in a memory means of the copy management apparatus. Alternatively, the encryption means may include encryption key and/or decryption key generating means for generating at least

one encryption key and/or decryption key.

The above-described copy management apparatus for controlling the number of data player devices which may be used may be implemented in an Application Specific Integrated Circuit (ASIC). The ASIC may be incorporated in the copying system itself or may alternatively be provided as external hardware for connection between the copying system and the removable memory card or data player device.

Preferably, the encryption means, including the encryption key (and decryption key, where this is not the same) are held in an internal non-volatile memory means provided in the ASIC, which location is inaccessible to a user. The clock means, the monitoring means, the protection means and the memory means for storing said registration codes are also all preferably inaccessible to a user. In this manner the copy management apparatus may be made substantially tamper-proof.

In another possibility, the above-described copy management apparatus for controlling the number of data player devices may be implemented by processor means controlled by software or firmware code held in a memory means of the copying system.

According to another aspect of the invention we provide a data copying and playback system incorporating copy management, the system comprising:

copying means for copying digital data from a first data storage means accessible to the copying means in use thereof to at least one second data storage means provided as part of the copying and playback system;

at least one data player device for playing back data (for example, text or music) stored on an associated said second data storage means, each said player device having a respective registration code and a respective private key stored in a first memory means provided in the player device;

second memory means associated with the copying means for

storing up to a predetermined maximum number of said registration codes, each code being associated with a respective said player device;

encryption means for encrypting data copied from the first data storage means, including an encryption key for use in carrying out the data encryption, and including encryption means for encrypting a decryption key provided in the copying means using each said registration code which is stored in the second memory means, in order to generate a respective encrypted decryption key for each said stored registration code;

clock means for measuring the passing of a finite predetermined period of time within which new registration codes are prevented from being written to the second memory means;

monitoring means for monitoring the number of registration codes stored in the second memory means and starting said clock means when said monitoring means detects that the predetermined maximum number of codes have been stored;

protection means for setting the second memory means in a protected mode, in which new registration codes are prevented from being stored therein, while said clock means measures the passing of said finite period of time;

registration handler means for receiving at least one said registration code uploaded, directly or indirectly, from at least one said data player device, comparing said at least one uploaded registration code with the registration codes already stored in the second memory means, storing said at least one uploaded registration code in the second memory means if the second memory means does not already contain said at least one uploaded registration code and the memory means does not already contain said predetermined maximum number of registration codes, and preventing said uploaded registration code from being stored in the second memory means if the second memory means is set in said protected mode; and

data transfer means for transferring the encrypted data to at least one said second data storage means, together with each

said encrypted decryption key;

decryption means provided in each said player device for decrypting the encrypted data transferred to said second data storage means, and including decryption means for decrypting the encrypted decryption key using the respective private key for the said player device;

digital to analogue converter means for converting the decrypted digital data into an analogue data signal for a user to playback; and

playback means for playing the decrypted analogue data signal to a user, for example via speakers or headphones (where the analogue data signal is music), or via a visual display screen (where the analogue data signal is text).

The second data storage means preferably comprises a removable solid state memory card formed and arranged for interfacing with the player device and with the copying means. In use, the registration code stored in the first memory means, in the player device, may be uploaded therefrom to the memory card which may then be interfaced with the copying means for uploading the registration code into the second memory means associated therewith.

Alternatively, the second data storage means comprises solid state memory means incorporated in the player device, and the player device is formed and arranged for interfacing to the copying system to enable the registration code stored in the first memory means in the player device to be uploaded therefrom to the registration handler means which may, for example, be provided in an interface means of the copying means. In this case, the first memory means may be provided in the second data storage means in the player device or may be provided as a separate memory in the player device.

The decryption means and the D/A converter means are preferably provided in an ASIC incorporated in the player device. In this way, no data will appear outside the ASIC in

an unencrypted form, except in an analogue data signal (e.g. music) for user playback.

Preferred embodiments of the invention will now be described by way of example only and with reference to the accompanying drawings in which:

Fig.1 is a schematic illustration of the main components of an audio copying and playback system, incorporating a copy management scheme according to the invention;

Fig.2 illustrates four basic steps involved in a copy management scheme based on the use of removable memory cards;

Fig.3 illustrates two basic steps in a modified copy management scheme involving only a copying station or unit and portable player device(s);

Fig.4 is a detailed block diagram illustrating data transfer operations between a removable memory card and a portable audio player device;

Fig.5 is a detailed block diagram illustrating data transfer operations between the removable memory card of Fig.2 and an audio dubbing station;

Fig.6 is a flow diagram illustrating the main operational steps carried out to uploading a registration code from the player device to the removable memory card of Fig.4;

Fig.7 is a flow diagram illustrating the main operational steps carried out to transfer data from the audio dubbing station to the removable memory card of Fig.5; and

Fig.8 is a flow diagram illustrating the main operational steps carried out to transfer and playback data from the removable card using the player device of Fig.4.

Fig.1 shows a copying system in the form of a unit 1 which may be used to copy audio data onto solid state memory from which the audio data can be played back to a user, remotely from the copying unit 1, using a player device 2. The copying unit 1 may, for example, be a dubbing station specially designed for receiving one or more Compact Discs (CDs) and copying audio data therefrom onto solid state memory. Such a dubbing station

is described in our British Patent Application No. 9825338.8 filed 19 November 1998, entitled "Audio Dubbing System". Alternatively, the copying system may comprise a PC with a CD-ROM drive or network access to, for example, the Internet, or a set-top box unit via which a user may purchase and download audio data (e.g. from a cable supplier). The player device 2 may be a portable audio player designed to interface to a removable solid state memory card 3 having FLASH or DRAM memory 5, which card 3 can be engaged in the copying unit 1 and having an interface 4 for enabling digital audio data copied (e.g. from a CD) by the copying unit to be downloaded onto the card 3. Alternatively, the FLASH or DRAM memory 5 may be incorporated in the player device 2 itself which is provided with an interface 4 for interfacing to the copying unit 1. The copying unit 1 includes encryption means 7 for encrypting digital data to be copied onto the FLASH/DRAM 5. The encryption means comprises encryption software, using known encryption algorithms, programmed into a memory of a processor means provided in the copying unit. Suitable encryption algorithms are described in the following references, although these shall not be taken to be exclusive (other encryption algorithms may also be suitable): (1) A S Tanenbaum, "Computer Networks", 1989, Prentice-Hall Inc, USA, Second Edition (2) R L Rivest, A Shamir and L M Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, 21(2): 120-126, Februray 1978 (3) [RY97], M Robshaw and Y Yin, "Elliptic curve cryptosystems", RSA Laboratories Technical Note, Revised June 27, 1997.

The player device 2 includes a decoder 6 in the form of decryption software, or dedicated decryption hardware, for decrypting the encrypted data downloaded to the FLASH/DRAM, as well as an interface 8 for interfacing the decoder 6 with the FLASH/DRAM 5. The player device 2 also includes a D/A converter 9 for converting decrypted digital data into analogue audio, which a user may listen to via headphones 10.

Fig.2 illustrates four steps carried out during operation of the apparatus of Fig.1, where a removable memory card 3 is used. In Step 1, a user registers one or more different player devices 2 (e.g. a portable player, car player unit and a home stereo unit incorporating solid state memory) with the memory card 3, by uploading a respective registration code 20 stored in each player device 2 (stored in substantially tamper-proof memory in the player devices 2), into the memory card 3. In Step 2, the registration code(s) are uploaded from the card 3 into a memory of the copying unit 1 (e.g. dubbing station or vending unit/set-top box). Each registration code is only uploaded if: (1) the memory does not already contain said registration code; (2) the memory does not already contain a predetermined maximum number of stored registration codes of player devices; and (3) the memory is not set in a protected state in which new registration codes are prevented from being written to the memory.

In Step 3, encrypted audio data is transferred from the copying unit 1 to the memory card 3, together with one or more encrypted versions of a decryption key, which in this embodiment is the same key as the encryption key which was used to encrypt the audio data. (This key shall hereinafter thus be referred to a the encrypt/decrypt key.) The encrypt/decrypt key is encrypted once using each registration code stored in the memory of the copying unit 1, so as to produce one or more different encrypted versions of the encrypt/decrypt key. In Step 4, the card 3 is interfaced with the player device 2 (via a dedicated interface 90 of the player) which extracts the encrypted data from the card 3, including a relevant one of the encrypted versions of the encrypt/decrypt key, and decodes the encrypted data using the encrypt/decrypt key which the player device decodes first, using a private key, held in the player for this purpose. The decoded audio data is converted to analogue form in the player device for playback to a user.

Figs.4 and 5 illustrate in more detail the key components of a hardware embodiment of the copy management scheme, and the data transfer operations carried out therebetween. Figs.4 and 5 show an audio system incorporating a "base unit" 1 which delivers data from a data source 22 to a removable FLASH card 3. The data source 22 may a copying unit as afore-described for copying data from, for example, a CD or DVD, or may be a memory (such as a hard disk) to which data has already been copied (e.g. from a CD using a copying unit, or downloaded from the Internet). Integrated circuitry containing various components, which will be described in further detail below, is contained in the base unit 1 (preferably in an Application Specific Integrated Circuit (ASIC), for implementing the copy management scheme. A removable FLASH card 3 (of any convenient known type) is provided for interfacing with the base unit 1, via a memory card interface 25 for receiving data therefrom, and for interfacing with one or more player devices 2 (only one shown in Fig.4). The ASIC in the base unit 1 incorporates an encryption module 26, a registration handler module 27, a non-volatile memory 28 for storing registration codes, a random encrypt/decrypt key generator module 29, an internal clock 30, and a counter unit 31 (incorporating the clock 30) in which a counter value 32 is stored in volatile memory 33 therein. The non-volatile memory 28 contains memory locations for holding a write flag 34 (for indicating that the non-volatile memory 28 is in write-protected mode). The non-volatile memory 28 also contains a write counter (not shown) which generates a write count 35, as will be described herebelow. The base unit 1 also has an interface 24 for interfacing with the removable memory card 3.

The player device 2 also contains an ASIC containing a decoder module 36, a D/A converter 38, and a non-volatile memory 39 holding a registration code or "key" 37 for the player device, as well as a private key 42 for the player device. The player has an output 40 for connection to an audio output means e.g.

headphones (not shown). The card 3 incorporates memory 60 containing a dedicated set of memory locations 45 for holding up to a predetermined maximum number of registration codes 20, the remainder of the memory locations in the card 3 being available for storing: encrypted data 50,51 downloaded from the base unit 1; up to a predetermined maximum number of sets (in Fig.4, up to at least three sets 52,53,54) of encrypted decryption key(s) 52,53 downloaded from the base unit (there being enough storage space available for up to a predetermined maximum number of such encrypted decryption keys in each set), each encrypted decryption key being stored on the card, together with the respective player registration key 37 corresponding thereto; and for storing Table of Contents (TOC) information 55 (optional). The card 3 may also incorporate a controller 62 for controlling the interfacing of the card 3 with the interfaces 25, provided in the player device(s) 2 and the base unit 1.

The remaining components of the base unit 1 and the player device(s) 2 will be described with reference to the operation of the whole system as follows. Figs.7, 8 and 9 also illustrate, in flow diagram form, the sequence of described operational steps.

(A) Player registration (to Card)

As illustrated in Fig.7, the first step in the process, once the card 3 has been connected/interfaced to a player 2, is to retrieve the list of player registration keys (if any) already stored on the card 3. If any of these stored registration keys match the registration key of the player which a user is attempting to register on the card 3, the registration process is ended, with no registration key being uploaded from the player to the card (since that player's key registration key is already stored on the card 3). If none of the already stored registration keys match, a checking operation is carried out (by a registration handler module 70 provided in the player 2, via the card controller 62, if any) to see if there is memory space available in the specified memory 45 of

the card 3 to store the new registration key 37. If there is space, the new registration key is uploaded (i.e. copied to) the card 3, by the registration handler 70, from the non-volatile memory in the player. If there is not enough space available, the user is notified, via a user interface provided in the player 2, that there is not enough space. (The user may be given the option to delete, or overwrite, an existing registration key stored on the card 3, in order to allow the new registration key to be uploaded.)

(B) Transfer of Data from Base Unit to Card

Fig.8 illustrates in flow diagram form the following described steps, which are carried out by the registration handler 27 in the base unit 1:

Check that card 3 is connected/interfaced to base unit 1 (card interface 24 thereof.) If not connected, request user (via user interface on base unit 1) to connect card 3. If card 3 is connected, compare registration key(s) 20 stored in card 3 with those already stored (if any) in the non-volatile memory 28 of the base unit. If there are no matches, check to see if the write flag 34 is enabled (set to 1). If it is, this indicates that a new registration key can be written, so registration handler 27 uploads (i.e.copies) a new registration key from the list stored on the card 3, in the non-volatile memory 28 of the base unit 1 (by adding it to the next empty registration key store 21 provided in the memory 28, or otherwise overwriting stored keys in circular fashion), and adds one to the write count 35 stored in the same memory 28 of the base unit 1. The registration handler 27 checks to see if the maximum allowed write count has now been reached (by comparing the write count with a predetermined maximum value also stored in the non-volatile memory 28) and if it has, the counter 33 in the counter unit 31 is reset (so as to start counting up to a predetermined count value) and the write flag is disabled (by resetting the bit to zero). If the maximum write count has not been reached, the next new registration

code will be uploaded from the card 3 in the same way as the previous one, and this process will continue until the maximum write count is reached (or there are no more new registration keys to be uploaded).

The clock 30, internal to the counter unit 31, is a free running oscillator linked to the counter 33 which, once started, is set to count up to a predetermined threshold value. While the counter 33 is counting up to this threshold count value the write flag remains disabled (i.e. binary bit is set to zero) in memory 28 so that the memory 28 is set in PROTECTED mode whereby no new registration keys can be written thereto. The count value thus determines the predetermined period of time (e.g. 24 hours) which must pass before the write flag is reset. Once this set time period has elapsed the clock counter 33 is reset and the write flag 34 enabled (i.e. binary bit switched to one) to indicate that the non-volatile memory 28 is now in ENABLED state in which new registration codes may be written thereto.

The counter unit 33 is implemented in an SRAM which is powered by a battery. If the battery is taken out, the count value 32 (stored in volatile memory) is reset (i.e. all bits of count are reset back to zero). So, while battery power is available, the counter counts up until it reaches a predetermined threshold value. A counter test module 72 is incorporated in the counter unit 31 which constantly compares the count value with a threshold count value stored therein and which, when this threshold value is reached, switches a binary digit (i.e. the write flag 34) stored in the non-volatile memory 28 of the base unit 1 to one, indicating that new player(s) 2 can again be registered. Because the count value 32 is stored in volatile memory, if the battery is removed before the counter reaches the predetermined threshold count, then the counter resets to zero and counts back up from zero again when the battery power is applied again.

While the write flag is disabled, the memory 28 is in PROTECTED status. In this protected status, the registration handler 27 will disallow any more registration codes to be written to the non-volatile memory 28 of the base unit. If the write flag 34 is enabled, the memory 28 is in ENABLED state and registration keys are allowed to be uploaded thereto.

Once all new registration codes which are allowed to be uploaded into the base unit 1 have been uploaded, the next step is the transfer, to the memory card 3, of data delivered from the data source 22. This is achieved by the following process:

a) Data is delivered from the data source 22 to the encryption module 26 via a data source interface 74 in the base unit 1;

b) Separate Encryption and Decryption keys are generated in the base unit 1 by a random encrypt and decrypt session key pair generator 29 (in two alternative possible embodiments, the Encryption and Decryption keys are selected from a preset internal list stored in the ASIC of the base unit 1, or a single encrypt/decrypt key is generated and used for both encryption and decryption). An additional encryptor 78 in the base unit 1 uses the player registration keys stored in location 21 of the non-volatile memory 28 to encrypt the randomly generated decryption key, which results in several different respective encrypted decryption keys 54. The generated encryption key is used to encrypt all the data delivered to the encryption module 26 from the data source 22 in one "session" (where one session is one data download operation e.g. downloading the contents of one CD). The encrypted data 56, and encrypted keys, are passed through a data formatter 80 in the base unit which formats the data into a suitable form for transferring to the memory card 3. The formatter 80 attaches these encrypted decryption keys to the encrypted data 50,21, for example in the form of a header, together with the

respective player registration key 37 for each encrypted decryption key, before transferring this information, as a data file F3 (for this one session), via the interface 24, to the card 3 connected thereto (via the controller 62 thereof, if any) as illustrated schematically in Figs.4 and 5.

In Figs. 4 and 5 the card 3 already carries two other data files F1, F2 containing encrypted data and encrypted decryption keys transferred to the card 3 in two previous "sessions". A different encryption key and decryption key pair is randomly generated for each session by the random session-key-pair generator 29.

(C) Playback Operation (Card to Player data transfer)

Fig.8 illustrates the series of steps carried out in order to playback data stored on the card 3, using the player device 2. With the card 3 connected to the card interface 90, a key look-up module 92 in the player 2 looks up the registration keys 37 stored in the or each data file F1,F2,F3 stored on the card 3, and compares these with the player's own registration key 37. If there is no match, the user is informed, via a user interface in the player, that access to the data on the card is restricted (i.e. forbidden) to this player device 2. If a match is found, the corresponding encrypted decryption key 54 is downloaded from the card and is decrypted (by a decryption module 94 in the player device) using the private key 42 stored in the player device 2 for this purpose. The encrypted data 56 (from the same data file F3 as the encrypted decryption key) is downloaded from the card 3 and decrypted (by the data decryption module 36) using the decrypted decryption key.

The decrypted audio data is converted to an analogue waveform by the D/A converter 38 in the player 2, and sent to the output 40 of the player, via an amplifier 96.

It will be appreciated that the player private key 42 is never transmitted outside the player device. By using tamper-proof non-volatile memory 98 to store the private key 42 in the player, the whole encryption/decryption system is made very secure. The registration key of the player is preferably also stored in the tamper-proof memory 98.

It will be appreciated that in the above embodiments, the audio data which is delivered from the base unit 1 to the encryption module 26 will generally be compressed audio data. The data compression may, for example, have been carried out during the copying of the data from a CD or DVD (using a copying system or unit), or the data may have been downloaded, in compressed form, from the Internet. Alternatively, it would though be possible for the data compression and encryption to be carried out together in the base unit 1 using a single compression/encryption algorithm to carry out both compression and encryption simultaneously, in the base unit 1. It will be appreciated that the decoder provided in the player device 2 will therefore also incorporate complementary decompression means for decompressing the decrypted audio data, or combined decompression/decryption means.

Although only one memory card 3 and one player device 2 are shown in the drawings, it will be appreciated that many different memory cards 3 could be used, each in the same manner as the above-described card 3. Also, the system is generally intended for use with two or more player devices 2 e.g. portable player, home stereo unit, car stereo unit etc., each having its own different registration code.

The player(s) 2 and/or the base unit 1 may be provided with means to allow a user to delete data (e.g. encrypted audio data, stored registration keys and encrypted decryption keys) from the memory card(s) 3, in order to allow new data to be stored (and new players registered with the card(s)). Also, a

facility may be provided to enable the user to rearrange the order of stored player registration keys.

Furthermore, the registration keys may include code which identifies a player as a certain type of player e.g. portable player, car player, and the system may be configured so as not to allow more than one of any said type of player to be registered with the base unit 1 at one time.

In any of the above-described embodiments, the registration handler 27 in the base unit 1 may incorporate a user interface for enabling a user to input manually (to the registration handler 27) the player registration codes, rather than these having to be uploaded directly from the player(s) 2 or card(s) 3. Although this system could thus be implemented without having to permanently store the player registration codes in the player(s) 2, preferably such a manual input facility would be provided as an additional feature of the system rather than as a replacement for the above-described system in which registration keys are stored in the player(s) and are loaded onto the card(s) 3, or into the base unit 1, directly from the player(s).

It will further be appreciated that various modifications to the above described embodiments are possible without departing from the scope of the invention. For example, Fig.3 illustrates an alternative audio copying and playback system in which, instead of using removable memory card(s) 3, the solid state memory onto which the audio data is delivered by the base unit 1 is incorporated permanently inside each player device 2, which in this case are portable audio player device(s). The system operates in exactly the same way as above-described with regard to the card/player/base unit system, with solid state memory provided in the player device performing all the functions/operations carried out by the memory card 3 in the above-described embodiment.

Also, it is possible that the data which is delivered from the data source 22 may already be in encrypted form e.g. if the data has been downloaded from a network supplier in encrypted form. In this case, the base unit 1 is provided with decryption means for decrypting this data, prior to encrypting it again using the encryption key provided in, or generated randomly, in the base unit 1. It is envisaged that it would be possible for an additional registration key/private key system similar to that described above (sometimes referred to as a "public key/private key" encrypt/decrypt system) to be used to control the decryption of such data by the base unit 1. This would involve the base unit 1 having its own registration code or key which is stored at the original data source (e.g. at the network supplier's end) and is used to decrypt encrypted data downloaded to the base unit.

It will also be appreciated that instead of using dedicated hardware such as ASICs, in the base unit 1 to carry out the above-described copy management operations, the base unit may incorporate a processor programmed with appropriate software and/or firmware, to carry out the necessary operational steps described with reference to the flow chart of Fig.7. Similarly, the or each player device 2 could incorporate a processor programmed with appropriate firmware (code) to carry out the registration handling, key look up and decryption functions.

CLAIMS

1. A method for controlling the number of data player devices (2) which may be used for playback of data which has been copied, using a copying system (1), from a first data storage means (22) accessible to the copying system in use thereof, to a second data storage means (3) associated with the player device(s), the method comprising the steps of:
providing a copy management means to which data copied from the first data storage means is delivered from the copying system (1);
providing a registration code (37) for each of a plurality of data player devices (2), said registration codes all being different;
providing a private key (42) for each of said data player devices, said private keys all being different;
storing a predetermined maximum number of said registration codes in a memory means (28) of the copy management means;
using an encryption key provided in the copy management means to encrypt data delivered to the copy management means from the copying system, and using each stored registration code to encrypt a decryption key provided in the copy management means, so as to provide a plurality of respective encrypted decryption keys;
transferring the encrypted data to a second data storage means (3) associated with at least one said player device, together with the plurality of encrypted decryption keys;
using the private key provided in said at least one player device to decrypt the respective encrypted decryption key, and using the decrypted decryption key to decrypt the encrypted data transferred to said second data storage means;
and preventing new registration codes from being stored in the memory means (28) of the copy management means until a predetermined time period has elapsed.

2. The method according to claim 1 wherein the decryption key provided in said copy management means is also the

encryption key used to encrypt the data being copied.

3. The method according to claim 1 wherein the decryption key stored in the copy management means is different to the encryption key.

4. The method according to any preceding claim wherein the private key (42) provided in each player device is the registration code (37) for the player device.

5. The method according to any of claims 1 to 3 wherein the private key (42) provided in each player device is different to the registration code (37) for the player device.

6. Copy management apparatus for controlling the number of data player devices (2) which may be used for playback of data which has been copied, using a copying system (1), from a first data storage means (22) accessible to the copying system in use thereof, to a second data storage means (3) associated with the player device(s), the apparatus comprising:
memory means (28) for storing up to a predetermined maximum number of registration codes (37), each said code being associated with a respective data player device (2);
encryption means (26, 78) for encrypting data delivered thereto, including an encryption key for use in carrying out the data encryption, and including encryption means (78) for encrypting a decryption key, provided in the apparatus, using each said registration code which is stored in the memory means (28) in order to generate a respective encrypted decryption key for each said stored registration code;
clock means (30, 33) for measuring the passing of a finite predetermined period of time within which new registration codes (37) are prevented from being stored in the memory means (28);
monitoring means (27, 35) for monitoring the number of registration codes stored in the memory means and starting said clock means when said monitoring means detects that the

predetermined maximum number of codes have been stored; protection means (34, 72) for setting the memory means in a protected mode, in which new registration codes are prevented from being entered in the memory, while said clock means (30, 33) measures the passing of said finite period of time; registration handler means (27) for receiving at least one registration code uploaded, directly or indirectly, from at least one said data player device (2), comparing said at least one uploaded registration code with the registration codes already stored in the memory means, storing said at least one uploaded registration code in the memory means (28) if the memory means does not already contain said at least one uploaded registration code and the memory means does not already contain said predetermined maximum number of registration codes, and preventing said uploaded registration code from being stored in the memory means if the memory means is set in said protected mode; and

data transfer means (24, 80) for transferring the encrypted data, together with each said encrypted decryption key, to a second data storage means (3) associated with at least one said player device.

7. Copy management apparatus according to claim 6 wherein the monitoring means comprises counter means (35) for counting the number of registration codes (37) which are written to the memory means.

8. Copy management apparatus according to claim 7 wherein the registration handler means (27) is formed and arranged to check the status of the counter means (35), upon receiving an uploaded registration code, and to allow or prevent the uploaded registration code from being written in the memory means (28) according to whether the counter means indicates that the memory means already contains said predetermined maximum number of stored registration codes or not, respectively.

9. Copy management apparatus according to any of claims 6 to 8 wherein the encryption key is selected from a predetermined list of encryption keys stored in a memory means of the copy management apparatus.

10. Copy management apparatus according to any of claims 6 to 8 wherein the encryption means includes encryption key generating means (29) for generating at least one encryption key.

11. Copy management apparatus according to any of claims 6 to 10 wherein the decryption key is also the encryption key.

12. Copy management apparatus according to any of claims 6 to 10 wherein the decryption key is selected from a predetermined list of decryption keys stored in a memory means of the copy management apparatus.

13. Copy management apparatus according to any of claims 6 to 10 wherein the encryption means (29) includes decryption key generating means for generating at least one decryption key.

14. Copy management apparatus according to any of claims 6 to 13 wherein the apparatus is implemented in an Application Specific Integrated Circuit (ASIC).

15. Copy management apparatus according to claim 14, wherein the ASIC is incorporated in the copying system (1).

16. Copy management apparatus according to claim 14, wherein the apparatus is provided as external hardware for connection between the copying system (1) and the second data storage means (3).

17. Copy management apparatus according to any of claims 14 to 16 wherein the encryption means (26), including the encryption key, are held in an internal non-volatile memory

means provided in the ASIC, which internal non-volatile memory means is inaccessible to a user.

18. Copy management apparatus according to any of claims 6 to 17 wherein the clock means (30, 33), the monitoring means (27, 35), the protection means (34, 72) and the memory means (28) for storing said registration codes are all inaccessible to a user.

19. Copy management apparatus according to any of claims 6 to 13 wherein the encryption means (26, 78), monitoring means (27, 35) and registration handler means (27) are implemented by processor means controlled by programming code held in a memory means of the copying system (1).

20. A data copying and playback system incorporating copy management, the system comprising:
copying means (1) for copying digital data from a first data storage means (22) accessible to the copying means in use thereof to at least one second data storage means (3) provided as part of the copying and playback system;
at least one data player device (2) for playing back data stored on an associated said second data storage means (2), each said player device having a respective registration code (37) and a respective private key (42) stored in a first memory means (98) provided in the player device;
second memory means (28) associated with the copying means for storing up to a predetermined maximum number of said registration codes, each code being associated with a respective said player device;
encryption means (26, 78) for encrypting data copied from the first data storage means, including an encryption key for use in carrying out the data encryption, and including encryption means for encrypting a decryption key provided in the copying means using each said registration code which is stored in the second memory means, in order to generate a respective encrypted decryption key for each said stored registration

code;

clock means (30, 33) for measuring the passing of a finite predetermined period of time within which new registration codes are prevented from being written to the second memory means;

monitoring means (27, 35) for monitoring the number of registration codes stored in the second memory means (28) and starting said clock means when said monitoring means detects that the predetermined maximum number of codes have been stored;

protection means (34, 72) for setting the second memory means in a protected mode, in which new registration codes are prevented from being stored therein, while said clock means measures the passing of said finite period of time;

registration handler means (27) for receiving at least one said registration code uploaded, directly or indirectly, from at least one said data player device, comparing said at least one uploaded registration code with the registration codes already stored in the second memory means, storing said at least one uploaded registration code in the second memory means if the second memory means does not already contain said at least one uploaded registration code and the memory means does not already contain said predetermined maximum number of registration codes, and preventing said uploaded registration code from being stored in the second memory means if the second memory means is set in said protected mode; and

data transfer means (24, 80) for transferring the encrypted data to at least one said second data storage means (3), together with each said encrypted decryption key;

decryption means (36, 94) provided in each said player device (2) for decrypting the encrypted data transferred to said second data storage means, and including decryption means (94) for decrypting a said encrypted decryption key corresponding to the said player device, using the respective private key (42) for the said player device;

digital to analogue converter means (38) for converting the decrypted digital data into an analogue data signal for a user

to playback; and

playback means (96, 40) for playing the decrypted analogue data signal to a user.

21. The data copying and playback system according to claim 20, wherein the digital data copied from the first data storage means (22) is digital audio data and the decrypted analogue data signal is an audio signal.

22. The data copying and playback system according to claim 20 or claim 21, wherein the second data storage means comprises a removable solid state memory card (3) formed and arranged for interfacing with the player device (2) and with the copying means (1).

23. The data copying and playback system according to claim 20 or claim 21, wherein the second data storage means comprises solid state memory means incorporated in the player device, and the player device is formed and arranged for interfacing to the copying system to enable the registration code stored in the first memory means (98) in the player device to be uploaded therefrom to the registration handler means (27).

24. The data copying and playback system according to claim 23 wherein the first memory means is provided in the second data storage means in the player device.

25. The data copying and playback system according to any of claims 20 to 24 wherein the decryption means (36, 94) and the D/A converter means (38) are provided in an ASIC incorporated in the player device (2).

26. The data copying and playback system according to any of claims 20 to 25 wherein each said data player device (2) whose registration code (37) is stored in said second memory means (28) is provided with identifier means for identifying the

said corresponding encrypted decryption key for the said data player device, from all of the encrypted decryption keys transferred to the second data storage means (3).

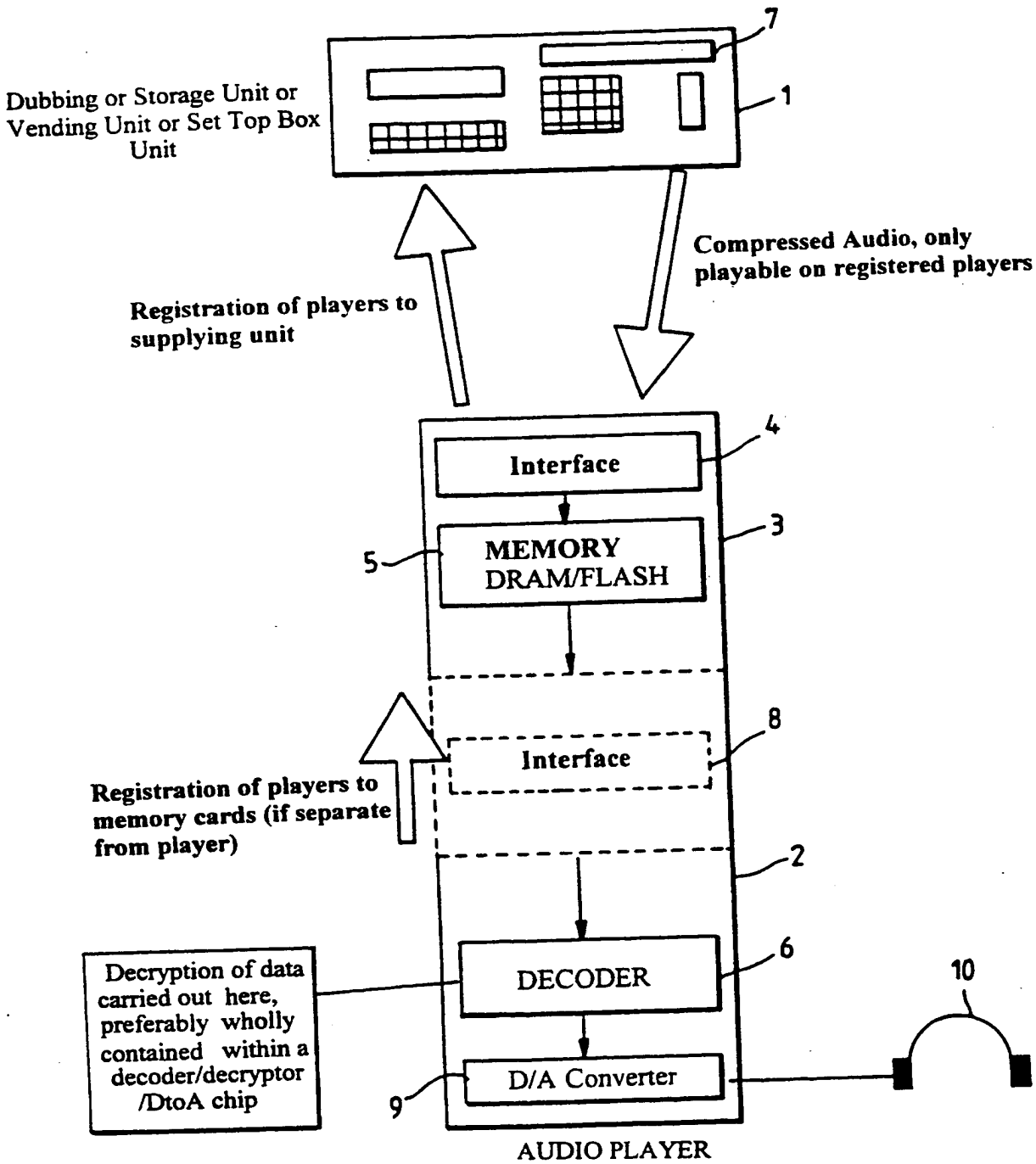


Fig. 1

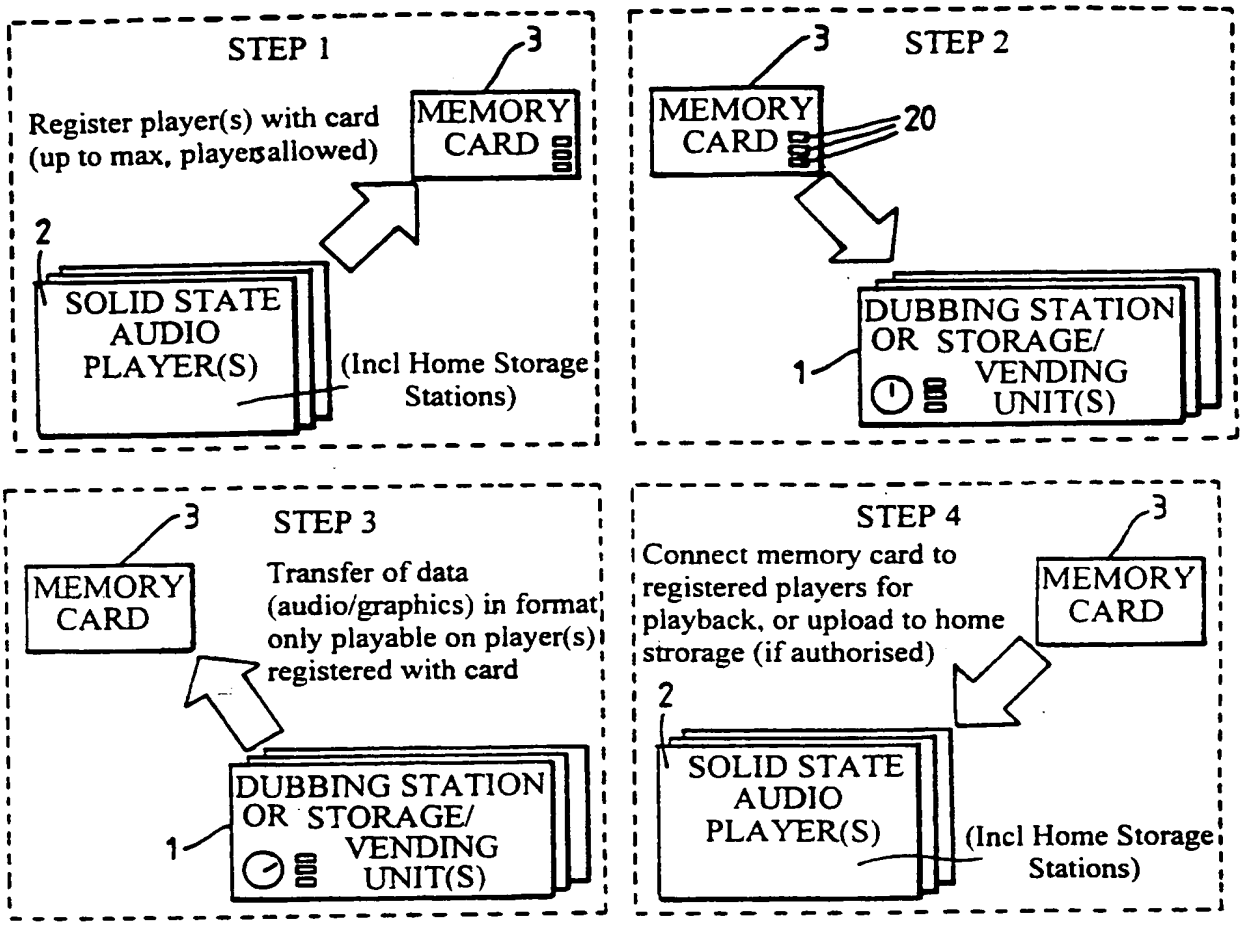


Fig. 2

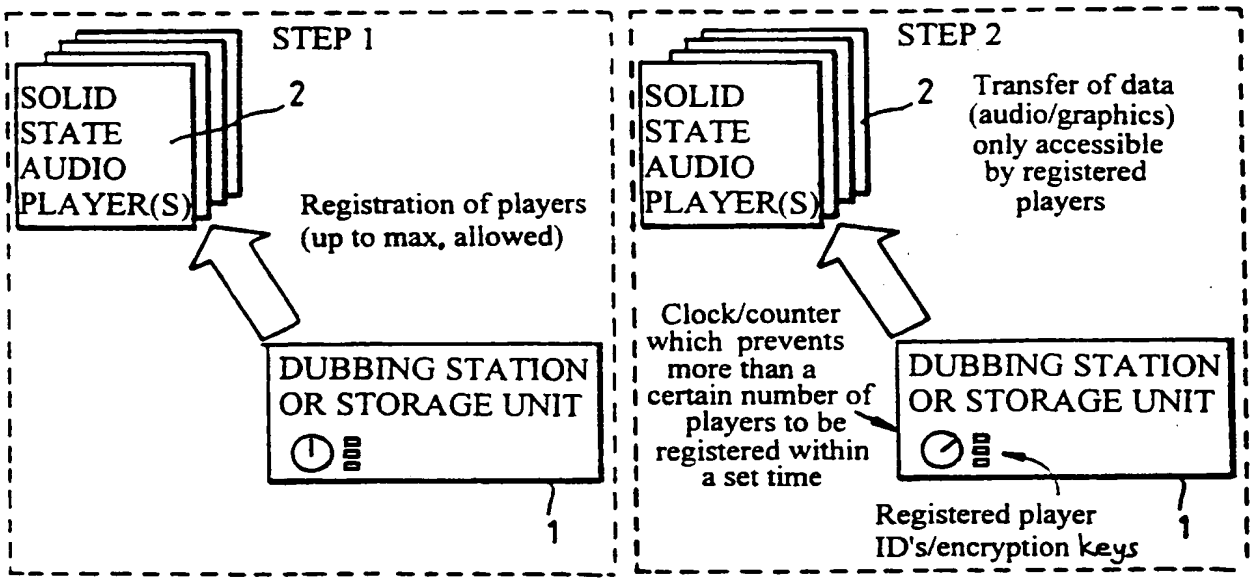


Fig. 3

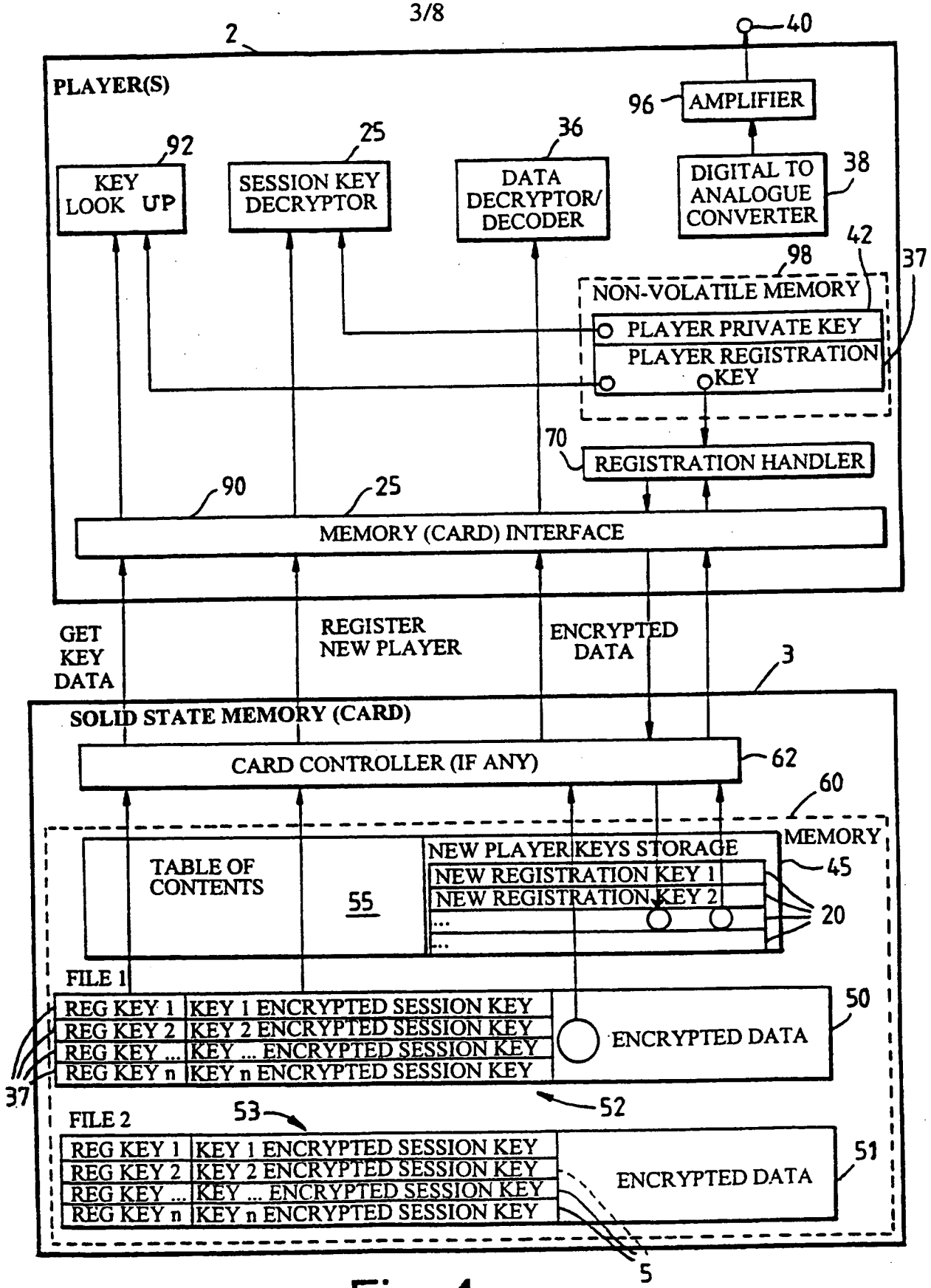


Fig. 4

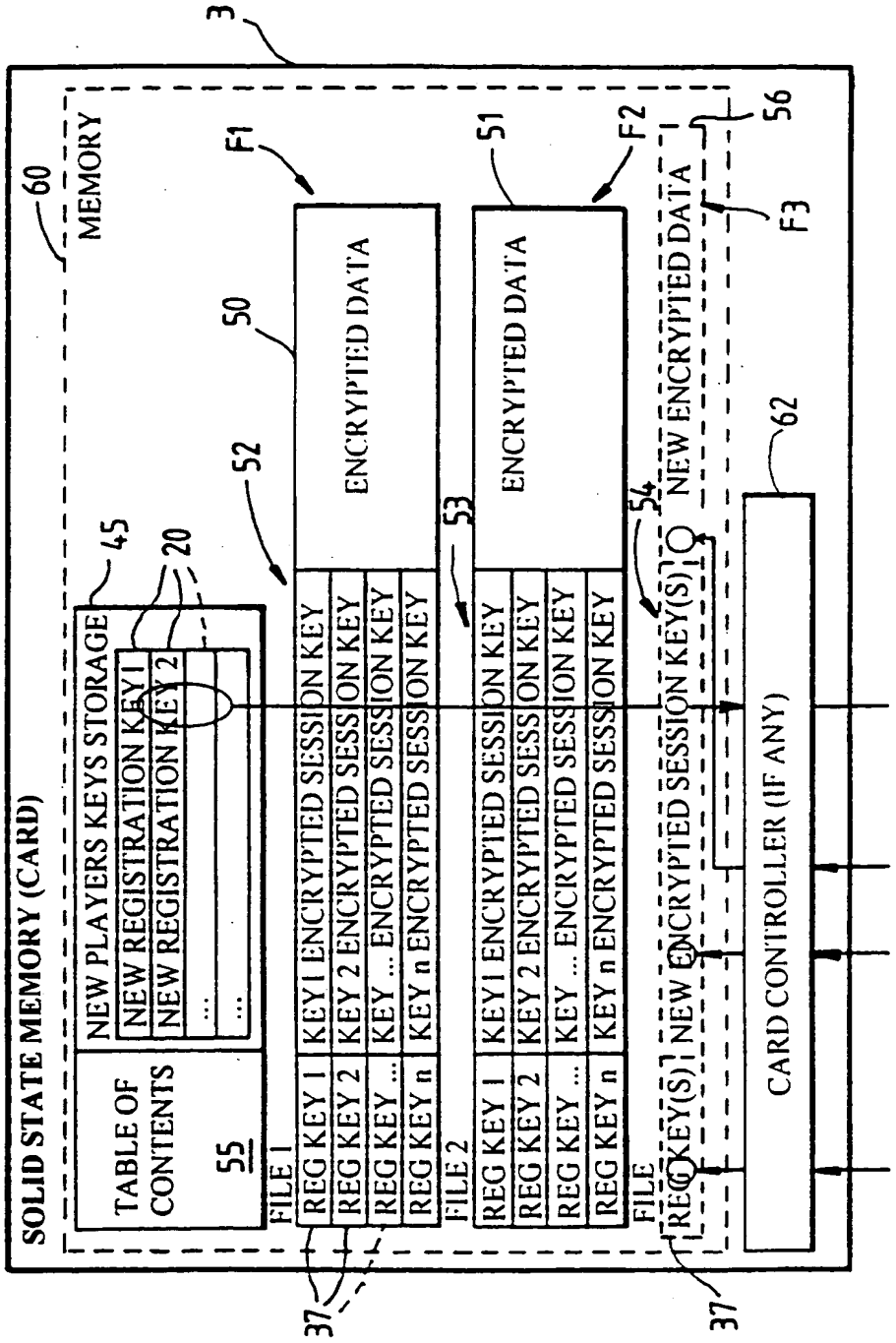


Fig. 5 (C'ntd)

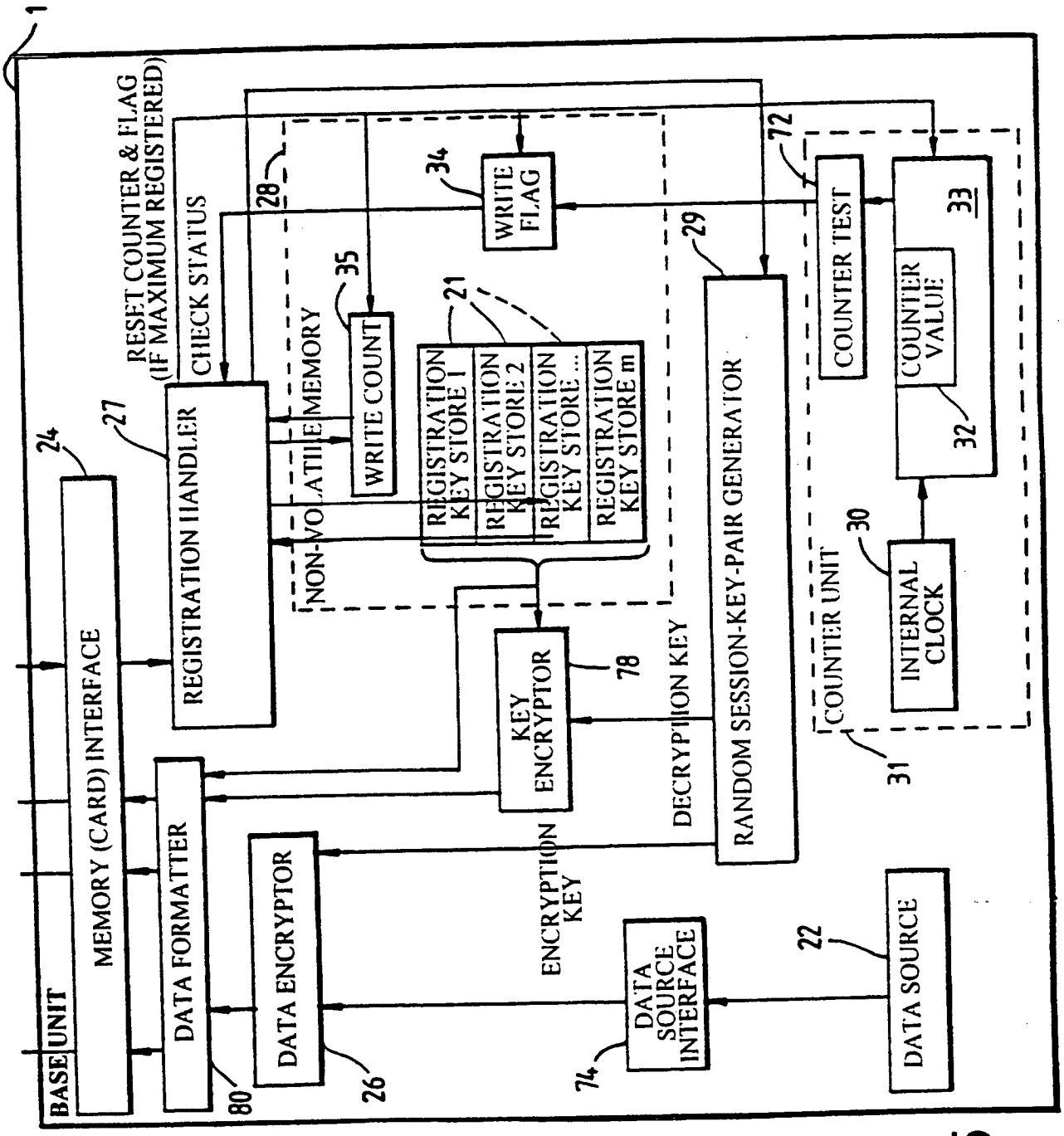


Fig. 5

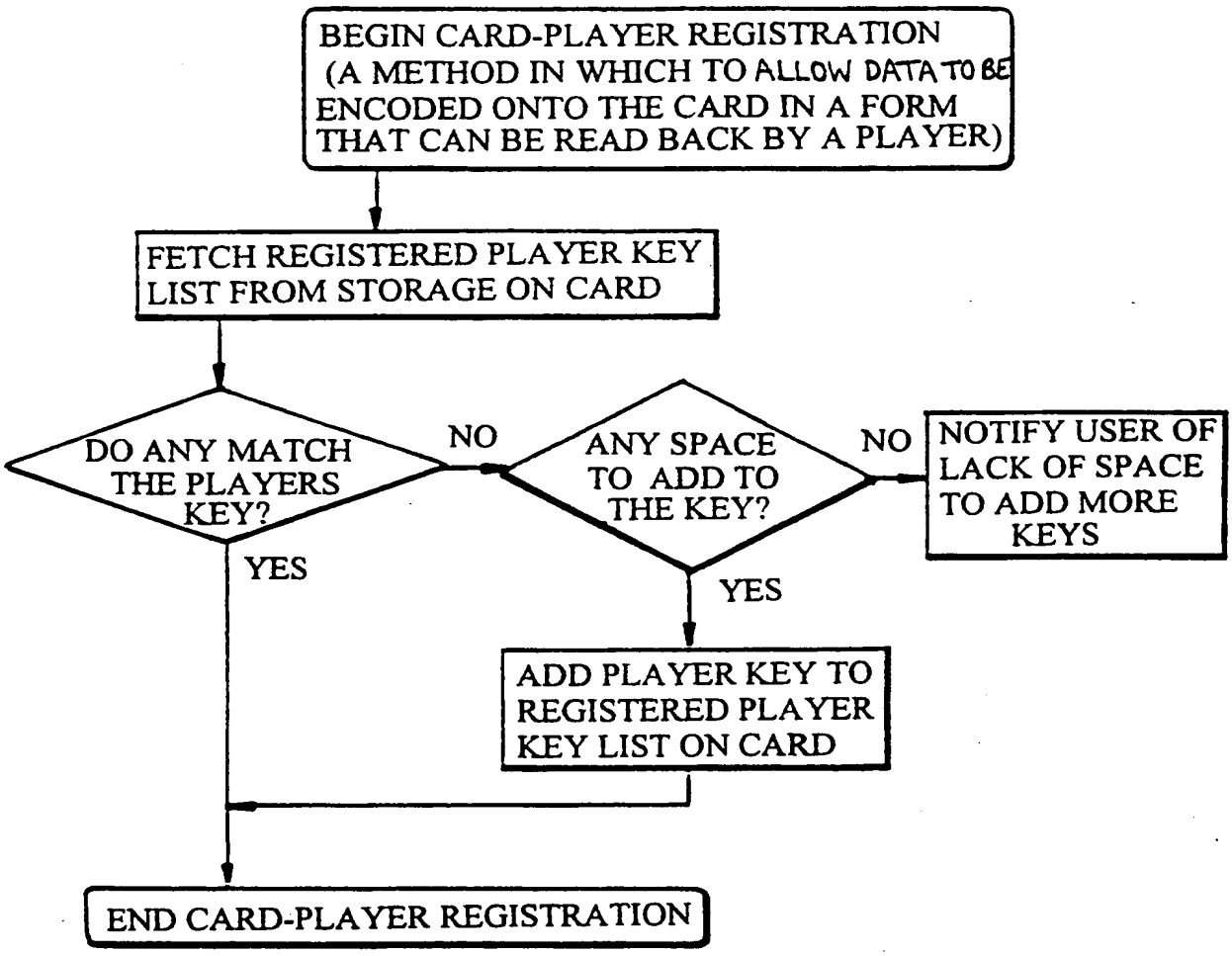


Fig. 6

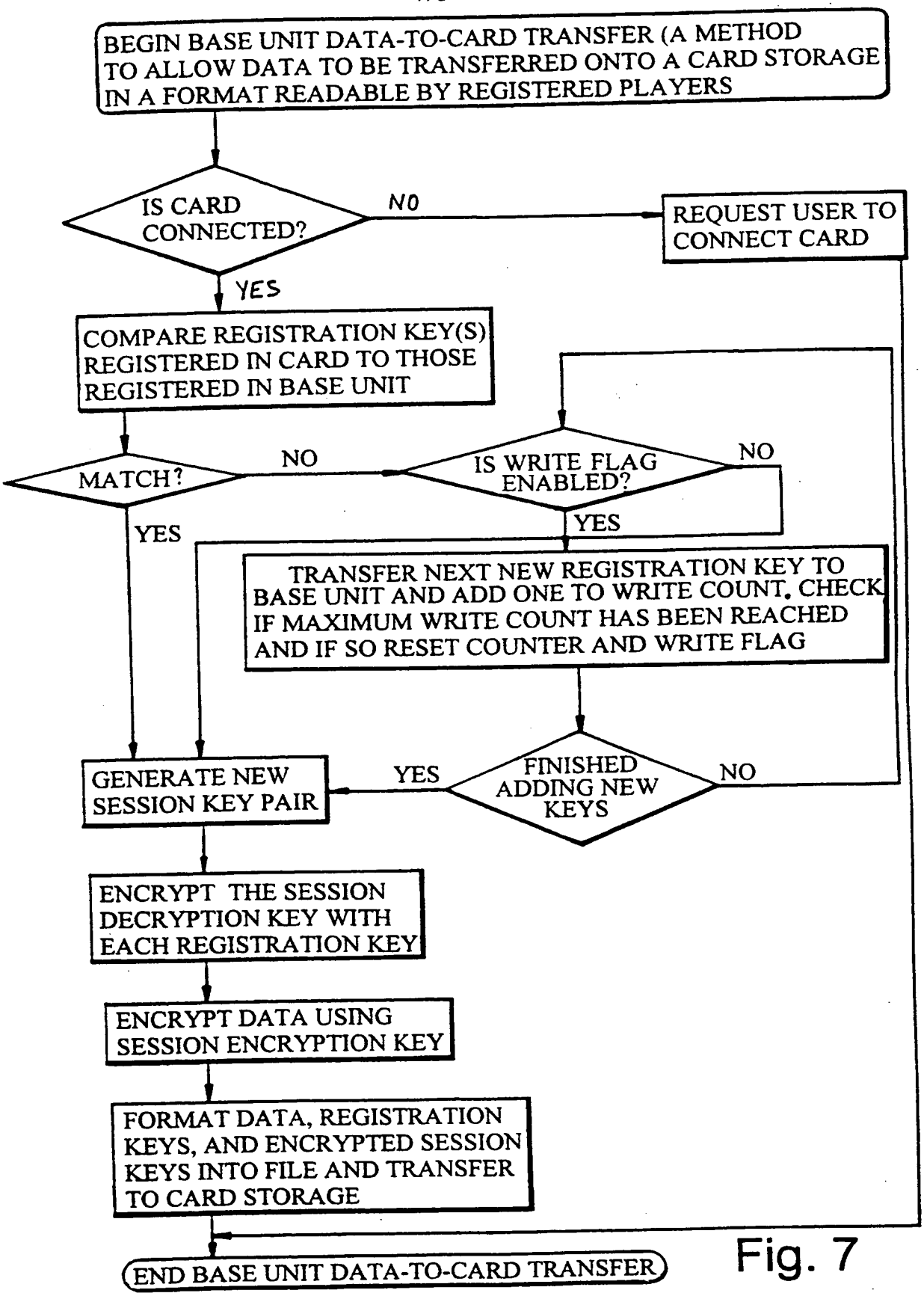


Fig. 7

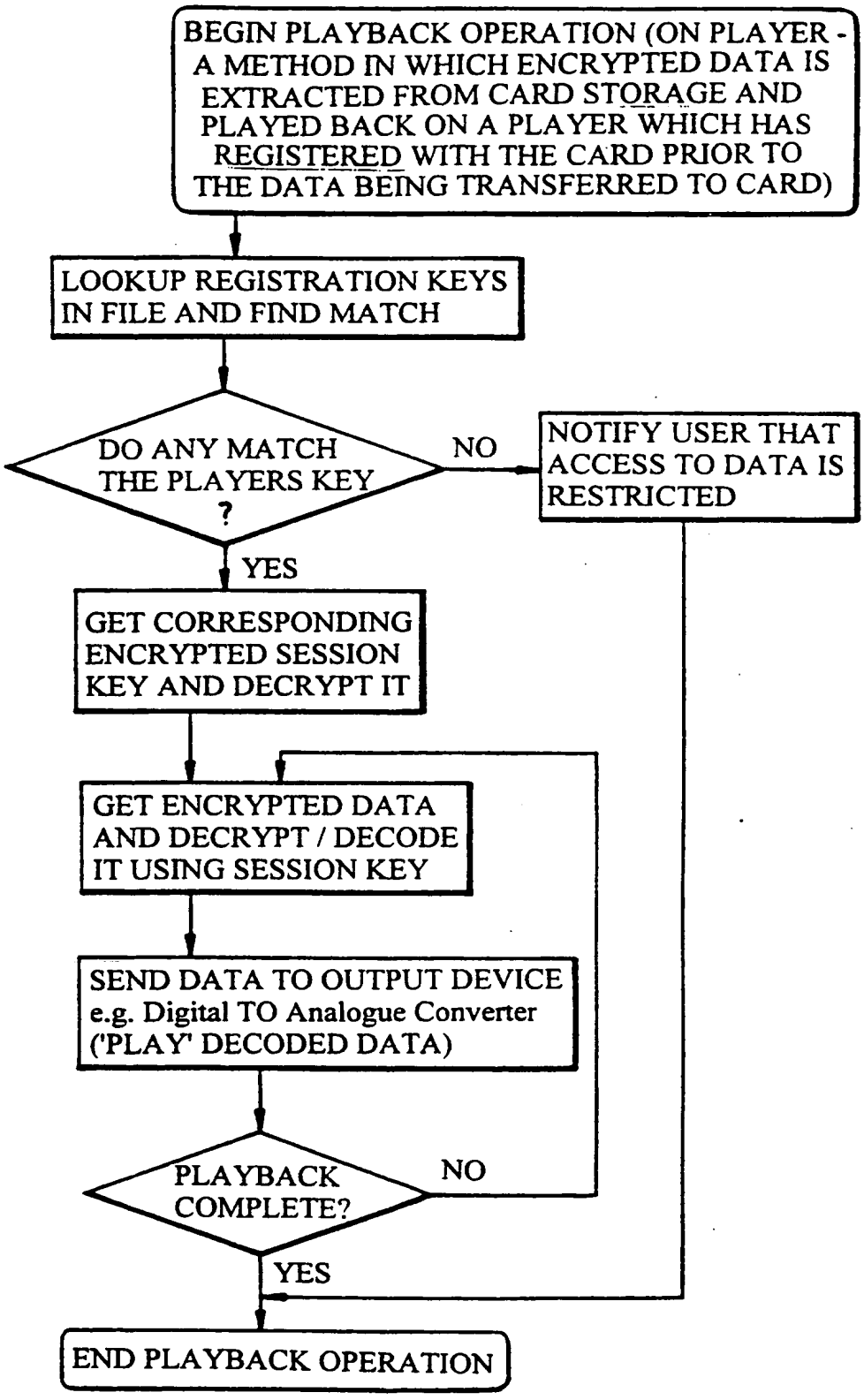


Fig. 8

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/GB 99/03877

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11C7/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11C G11B G06F H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 561 685 A (FUJITSU LTD) 22 September 1993 (1993-09-22) abstract column 2, line 18-20; figure 3	1,4-6,20
Y	WO 94 19886 A (GRUNDIG EMV ;ZELL HORST (DE)) 1 September 1994 (1994-09-01) the whole document	1,4-6,20

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 March 2000	17/03/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax (+31–70) 340–3016	Czarik, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

...ormation on patent family members

Interm ...al Application No
PCT/GB 99/03877

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0561685 A	22-09-1993	JP 5257816 A	08-10-1993
		US 5392351 A	21-02-1995
		US 5555304 A	10-09-1996
		US 5796824 A	18-08-1998
WO 9419886 A	01-09-1994	DE 4305960 C	24-03-1994
		AT 176836 T	15-03-1999
		DE 59309385 D	25-03-1999
		EP 0686328 A	13-12-1995
		ES 2127917 T	01-05-1999
		JP 8507617 T	13-08-1996
		US 5835588 A	10-11-1998